PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-196240
(43)Date of publication of application : 11.07.2003

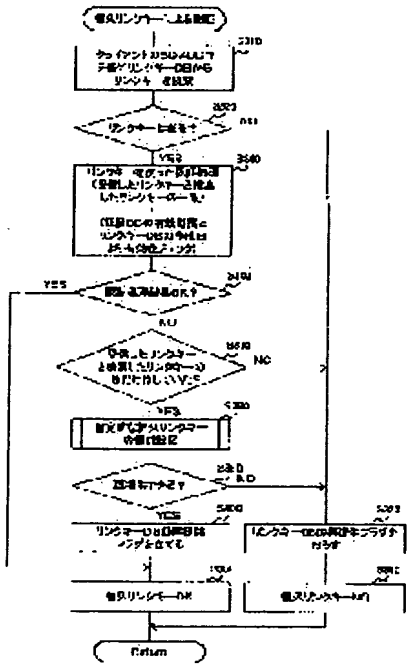
(51)Int.Cl. G06F 15/00
H04L 9/32

(21)Application number : 2001-400547
(22)Date of filing : 28.12.2001

(71)Applicant : BROTHER IND LTD
(72)Inventor : MATSUDA MAKOTO

(54) SERVICE PROVIDER, SERVICE PROVIDING SYSTEM, SERVICE PROVIDING PROGRAM, COMPUTER READABLE RECORDING MEDIUM WITH ITS PROGRAM RECORDED

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a service providing device capable of flexibly dealing with a service request.
SOLUTION: In this service providing system, a server 20 executes authentication processing to a client 10 based on a permanent link key acquired from a client 10 and a permanent link key registered in its own authentication DB (S340), and even when the client 10 is not authenticated by the permanent link key within the term of validity (S350: NO), as long as the client 10 is authenticated by the permanent key beyond the term of validity (S370: YES), a service is temporarily provided under a prescribed condition (S390: YES). Thus, it is possible to flexibly deal with the service request, and it is possible for a user side to easily use the service.



LEGAL STATUS

[Date of request for examination] 26.06.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

[0007]

Further, especially in the service providing device of claim 1, the temporary service providing means provides a temporary service even when the client device is not authenticated by the authenticating means, as long as the client device is a client device authenticated by the authenticating means in the past.

[0054]

As shown above, in this service providing system, the server 20 executes authentication processing to the client 10 based on a permanent link key acquired from a client 10 and a permanent link key registered in its own authentication DB (S340), and even when the client 10 is not authenticated by the permanent link key within the term of validity (S350: NO), as long as the client 10 is authenticated by the permanent link key beyond the term of validity (S390: YES), a service is temporarily provided under a prescribed condition (S390: YES). Thus, it is possible to flexibly deal with the service request, and it is possible for a user side to easily use the service.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－196240
（P2003－196240A）
(43)公開日　平成15年７月11日(2003.7.11)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｃ	５Ｂ０８５
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｚ	５Ｊ１０４

審査請求　未請求　請求項の数７　ＯＬ　（全９頁）

(21)出願番号　特願2001－400547(P2001－400547)

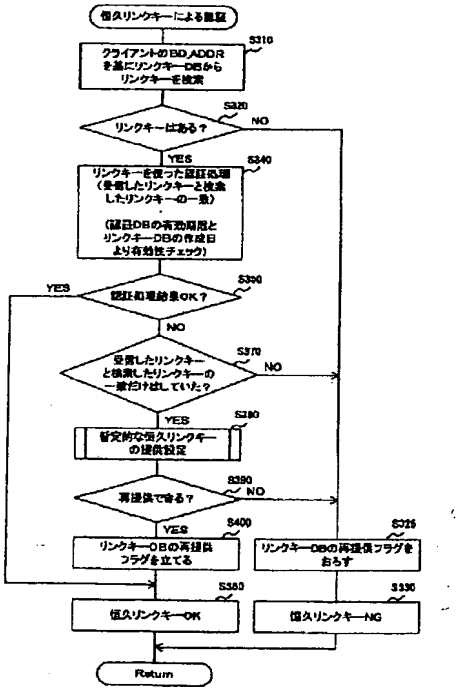
(22)出願日　平成13年12月28日(2001.12.28)

(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町15番１号
(72)発明者　松田　誠
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内
(74)代理人　100082500
弁理士　足立　勉　（外１名）

Ｆターム(参考)　5B085 AE03 AE04 BC02
5J104 AA07 KA02 PA07

(54)【発明の名称】　サービス提供装置、サービス提供システム、サービス提供プログラムおよび当該プログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　サービス提供装置において、サービス要求に対して柔軟な対応ができるようにする。
【解決手段】　本実施例のサービス提供システムにおいて、サーバ２０は、クライアント１０から取得した恒久リンクキーと自己の認証ＤＢに登録されている恒久リンクキーとに基づいて、クライアント１０に対する認証処理（Ｓ３４０）を行った結果、有効期限内の恒久リンクキーによってクライアント１０が認証されない場合であっても（Ｓ３５０：ＮＯ）、有効期限切れの恒久リンクキーによって認証される場合には（Ｓ３７０：ＹＥＳ）、所定の条件の下で、暫定的にサービスを提供する（Ｓ３９０：ＹＥＳ）。これにより、サービス要求に対する柔軟な対応が実現され、利用者側がサービスを利用し易くなる。



【特許請求の範囲】

【請求項１】照合情報を記憶する記憶手段と、クライアント装置から入手した認証情報と前記記憶手段に記憶された照合情報とに基づき、前記クライアント装置の認証を行う認証手段と、該認証手段によりクライアント装置が認証された場合に、サービスを提供するサービス提供手段とを備えたサービス提供装置であって、

前記認証手段によりクライアント装置が認証されない場合であっても、当該クライアント装置が、過去に前記認証手段により認証されたクライアント装置である場合は、暫定的なサービスを提供する暫定サービス提供手段を更に備えたことを特徴とするサービス提供装置。

【請求項２】前記記憶手段は、前記照合情報として、現在の及び過去の照合情報を記憶しており、

前記サービス提供手段は、前記認証手段を介して、前記クライアント装置から入手した認証情報と前記現在の照合情報とに基づいてクライアント装置が認証された場合にサービスを提供するとともに、

前記暫定サービス提供手段は、前記認証手段によりクライアント装置が認証されない場合であっても、前記認証情報と前記過去の照合情報とに基づいて当該クライアント装置が認証された場合は、暫定的なサービスを提供することを特徴とする請求項１に記載のサービス提供装置。

【請求項３】前記暫定サービス提供手段に基づく暫定的なサービスを提供する際に、所定の情報をクライアント装置に通知する通知手段を備えたことを特徴とする請求項１又は請求項２に記載のサービス提供装置。

【請求項４】請求項１乃至請求項３の何れか１項に記載のサービス提供装置において、

当該装置は複数のサービスを提供できるものであり、前記暫定サービス提供手段に基づく暫定的なサービスの提供可否が、該サービスごとに設定されていることを特徴とするサービス提供装置。

【請求項５】照合情報を記憶する記憶手段と、クライアント装置から入手した認証情報と前記記憶手段に記憶された照合情報とに基づき、前記クライアント装置の認証を行う認証手段と、該認証手段によりクライアント装置が認証された場合に、サービスを提供するサービス提供手段とを備えたサービス提供装置、としてコンピュータを機能させるためのプログラムであって、

更に、前記認証手段によりクライアント装置が認証されない場合であっても、当該クライアント装置が、過去に前記認証手段により認証されたクライアント装置である場合は、暫定的なサービスを提供する暫定サービス提供手段としてコンピュータを機能させるためのサービス提供プログラム。

【請求項６】請求項５に記載のサービス提供プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項７】クライアント装置と、照合情報を記憶する記憶手段と、クライアント装置から入手した認証情報と前記記憶手段に記憶された照合情報とに基づき、前記クライアント装置の認証を行う認証手段と、該認証手段によりクライアント装置が認証された場合に、サービスを提供するサービス提供手段とを備えたサービス提供システムであって、

前記認証手段によりクライアント装置が認証されない場合であっても、当該クライアント装置が、過去に前記認証手段により認証されたクライアント装置である場合は、暫定的なサービスを提供する暫定サービス提供手段を更に備えたことを特徴とするサービス提供システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、クライアント装置が認証された場合に、サービス提供を行うサービス提供装置、サービス提供システム、サービス提供プログラム及び当該プログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【０００２】

【従来の技術】従来より、クライアント装置が認証された場合にサービス提供を行うサービス提供装置においては、パスワードやリンクキー（後に後述する）などを入力させ、その入力されたパスワードやリンクキーが正規のものであるか否かを判断することによって認証処理を行っている。

【０００３】しかし、印刷サービス等もネットワーク化に伴い、利用する人が増加する傾向にあるため、中にはパスワードやリンクキーを何らかの方法によって盗みとり、不当にサービスの提供を受けようとする者がいる虞がある。この様な不安に対処するために、管理者としては、パスワードやリンクキーに有効期限を設けたり、定期的にそれらを変更することによってセキュリティを強化することが考えられる。

【０００４】

【発明が解決しようとする課題】しかしながら、セキュリティを強化するために、パスワードやリンクキーに有効期限を設けたり、定期的にそれらを変更することは有効であるが、有効期限が切れたことや、パスワードやリンクキーの変更に気付かず、以前のパスワードやリンクキーを用いてサービスを要求したユーザーには、サービスが提供されない。

【０００５】このようなユーザは、元々正規のユーザであるにも拘わらず、不当にサービスを受けようとする者を排除するために、突然サービスの提供が認められないといった不利益を与えていた。本発明はこうした課題を背景としてなされたものであり、サービス提供装置、サービス提供システム、サービス提供プログラム及び当該プログラムを記録したコンピュータ読み取り可能な記録媒体において、セキュリティを確保しつつ、サービス要求に対して柔軟な対応ができるようにすることを目的と

する。

【０００６】

【課題を解決するための手段及び発明の効果】上記課題を解決するためになされた請求項１記載のサービス提供装置においては、認証手段が、クライアント装置から入手した認証情報と、記憶手段に記憶された照合情報とに基づいて、クライアント装置の認証処理を行い、その結果、クライアント装置が認証された場合に、サービス提供手段がサービスを提供する。

【０００７】そして特に請求項１記載のサービス提供装置においては、認証手段によりクライアント装置が認証されない場合であっても、当該クライアント装置が過去に認証手段により認証されたクライアント装置である場合、暫定サービス提供手段が、暫定的なサービスを提供する。

【０００８】つまり、請求項１のサービス提供装置によれば、クライアント装置が認証されない場合であっても、サービス利用側は、暫定的ではあるがサービスを受けることができることとなる。即ち、サービス要求に対して柔軟な対応ができ、利用者側がサービスを利用し易くなるという効果を奏する。

【０００９】サービス提供を暫定的なものとすることは、例えば、サービス提供を一定期間に限定したり、サービス提供の回数を限定したりするなど、サービスを提供するための条件を定めておくことで実現できる。また、過去に認証手段により認証されたクライアント装置であるかどうかを判断できるようにするには、例えば、請求項２に記載の様にサービス提供装置を構成すればよい。

【００１０】即ち、請求項２に記載のサービス提供装置においては、記憶手段に、照合情報として、現在の及び過去の照合情報を記憶させており、サービス提供手段を、認証手段を介して、クライアント装置から入手した認証情報と現在の照合情報とに基づいてクライアント装置が認証された場合にサービスを提供するように構成している。そして、暫定サービス提供手段については、認証手段によりクライアント装置が認証されない場合であっても、認証情報と過去の照合情報とに基づいて当該クライアント装置が認証された場合は、暫定的なサービスを提供するよう構成している。

【００１１】この様に構成された請求項２に記載のサービス提供装置によれば、過去に認証手段により認証されたクライアント装置であるかどうかを判断することができる。ところで、暫定サービス提供手段によるサービス提供は暫定的なものであり、いつまでもそのサービス提供を受けることはできない。そこで、請求項３に記載の様に、暫定的なサービスを提供する際、通知手段に、所定の情報をクライアント装置に通知させるようにするとよい。この様にすれば、サービス利用側に対して注意を促すことができ、サービスがより利用しやすくなる。

【００１２】また、当該サービス提供装置が複数のサービスを提供できるものである場合には、請求項４に記載の様に、暫定サービス提供手段に基づく暫定的なサービスの提供可否を、サービス毎に設定しておくとよい。この様にすれば、サービス提供の運用により柔軟性を持たせることができる。

【００１３】なお、請求項５のサービス提供プログラム、および請求項６のコンピュータ読み取り可能な記録媒体によれば、コンピュータを、請求項１のサービス提供装置と同様に機能させることができ、この装置と同様の効果を得ることができる。また、請求項７に記載のサービス提供システムによれば、請求項１のサービス提供装置と同様の効果を得ることができる。

【００１４】

【発明の実施の形態】以下に、本発明の一実施例を図面と共に説明する。図１は、一実施例としてのサービス提供システム１の構成を示す図である。このサービス提供システムは、後述するリンクキーを記憶するための記憶部１２を有するクライアント装置（以下、「クライアント」という）１０と、サーバ装置（以下、「サーバ」という）２０とから構成されている。

【００１５】サーバ２０は、図２に示す様に、ＣＰＵ３０、ＲＡＭ４０、ＲＯＭ５０等からなるコンピュータ、入力装置６０、表示装置７０、通信装置８０、印刷装置９０で構成されており、ファクシミリ装置やプリンタ装置などとしての機能を備えた複合装置であって、プリントサービスやＦＡＸサービスなど、複数のサービスを提供できるものである。尚、サーバ２０は、請求項の「サービス提供装置」に相当する。

【００１６】ＣＰＵ３０は、制御部３２、演算部３４、データ比較部３６などから構成されており、ＲＯＭ５０に格納されたプログラムに基づいて所定の処理を実行するものである。ＲＯＭ５０には、請求項の「サービス提供プログラム」を構成する、認証制御プログラム５２やその他の動作プログラム５４が格納されている。

【００１７】ＲＡＭ４０には、認証データベース（ＤＢ）４２、サービスＤＢ４４、リンクキーＤＢ４６、各種動作用バッファ４８などの記憶領域が確保されている。認証ＤＢ４２は、データ項目として、図３（ａ）に示す様に、”認証の種類”、”認証の有無”、”有効期限”、”無効時の対応（回数）”および”無効時の対応（期限）”を有するデータベースである。

【００１８】またサービスＤＢ４４は、データ項目として、図３（ｂ）に示す様に、”サービス”、”認証の種類”、”ＰＩＮコード”および”恒久リンクキーの種類”を有するデータベースである。この”サービス”は、サーバ２０が提供可能なサービスである。

【００１９】またリンクキーＤＢ４６は、データ項目として、図３（ｃ）に示す様に、”恒久リンクキー”、”恒久リンクキーの種類”、”ＢＤアドレス”、”生成

日”、”再提供回数”、”再提供有効期限”および”再提供フラグ”を有するデータベースである。リンクキーＤＢ４６（具体的にはＲＡＭ４０）は、請求項の「記憶手段」として機能するものであり、”恒久リンクキー”が、請求項の「照合情報」に相当する。

【００２０】入力装置６０は、外部から入力操作を行うための入力部６２と、入力部６２に入力された情報をＣＰＵ３０に入力する入力制御部６４とを備えている。また、表示装置７０は、ＣＰＵ３０からの表示データを一旦蓄える表示制御バッファ７２と、表示制御バッファ７２に蓄えた表示データに基づく画像を表示部７４に表示させる表示制御部７６とを備えている。

【００２１】通信装置８０は、ＣＰＵ３０と通信データを送受する通信ポート８２と、アンテナ８４を用いて無線通信を制御する無線制御部８６とを備え、クライアント１０と通信可能に構成されている。クライアント１０およびサーバ２０は、Ｂｌｕｅｔｏｏｔｈ方式の無線通信によりデータの送受信を行う通信機器（ＢＴ通信機器）であり、他のＢＴ通信機器（本実施形態では、Ｂｌｕｅｔｏｏｔｈ方式の通信に対応したクライアント装置１０）との間で、Ｂｌｕｅｔｏｏｔｈ方式の無線通信を行う。Ｂｌｕｅｔｏｏｔｈ方式の通信では、通信開始時のリンクレイヤにおいて、リンクキーと呼ばれる秘密鍵を用いて接続認証が行われることにより、誤接続防止等のセキュリティが図られている。

【００２２】ＢＴ通信機器では、通信相手となる他のＢＴ通信機器毎に、そのＢＤアドレスと、２機器間で利用されるリンクキーとをペアにして記憶し管理するようになっている。例えば、本実施例のサーバ２０においては、リンクキーＤＢ４６に、クライアント１０のＢＤアドレスとリンクキーとをペアにして登録している。ここで、２機器間で利用されるリンクキーには、半固定的なリンクキーとしてのユニットキー及びコンビネーションキーと、一時的なリンクキーとしての初期化キーとがある。ユニットキーおよびコンビネーションキーは、機能的には同じものであるが、前者は単一のＢＴ通信機器の情報から生成されるものであるのに対し、後者は２つのＢＴ通信機器の情報を組み合わせて生成される点で異なる。

【００２３】通信相手についての半固定的なリンクキー（即ち、ユニットキー又はコンビネーションキー、以下、恒久リンクキーという）が既に設定されている場合には、そのリンクキーを用いて接続認証が行われるが、恒久リンクキーが設定されていない場合には、暫定的なリンクキーである初期化キーを生成する。

【００２４】ここで、初期化キーの生成方法について説明する。まず、初期化キーを生成しようとする２つのＢＴ通信機器（以下、機器Ａ及び機器Ｂとして説明する）において、接続要求を受けた側の機器Ｂが、当該機器Ｂで発生した乱数を接続要求側の機器Ａに送信する。また、各機器のＢＤアドレスは、通信の初期段階において交換されており、２機器間で周知のパラメータとなっている。

【００２５】そして、機器Ａは、当該機器ＡのＢＤアドレスと、当該機器ＡのＰＩＮコードと、機器Ｂで発生した乱数とから、初期化キー生成のための演算を行い、初期化キーを算出する。同様に、機器Ｂも、機器ＡのＢＤアドレスと、当該機器ＢのＰＩＮコードと、当該機器Ｂで発生した乱数とから、初期化キー生成のための上記演算を行い、初期化キーを算出する。尚、初期化キーを生成する場合、クライアント１０側においては当該クライアント１０のＰＩＮコードを入力する必要がある。

【００２６】一方、２つのＢＴ通信機器間の接続認証は、それぞれのＢＴ通信機器で通信相手について設定されているリンクキーが一致するか否かを判定することにより行われる。ここで、リンクキーが一致するか否かの判定方法について説明する。

【００２７】接続認証を行おうとする２つのＢＴ通信機器（以下、機器Ｃ及び機器Ｄとして説明する）において、認証要求を受けた側の機器Ｄが、当該機器Ｄで発生した乱数を認証要求側の機器Ｃに送信する。また、各機器のＢＤアドレスは、通信の初期段階において交換されており、２機器間で周知のパラメータとなっている。

【００２８】そして、機器Ｃは、当該機器ＣのＢＤアドレスと、機器Ｄについて設定されているリンクキーと、機器Ｄで発生した乱数とから、接続認証のための演算を行い、ＳＲＥＳと呼ばれるパラメータを算出する。同様に、機器Ｄも、機器ＣのＢＤアドレスと、機器Ｃについて設定されているリンクキーと、当該機器Ｄで発生した乱数とから、接続認証のための上記演算を行い、ＳＲＥＳを算出する。そして、機器Ｃは、当該機器Ｃで算出したＳＲＥＳを機器Ｄへ送信する。一方、機器Ｄは、当該機器Ｄで算出したＳＲＥＳと、機器Ｃから受信したＳＲＥＳとが一致するか否かを判定する。

【００２９】ここで、機器Ｄが、２つのＳＲＥＳが一致したと判定すると、接続認証が成立する。このように、接続認証では、セキュリティ確保のため、それぞれのＢＴ通信機器で通信相手について設定されているリンクキーが一致するか否かを、リンクキー自体を送信することなく判定するようになっている。

【００３０】なお、印刷装置９０は、ＣＰＵ３０から印刷データを受信する通信ポート９２と、ＣＰＵ３０から受信した印刷データを一時的に蓄える印刷制御バッファ９４と、印刷データに基づいて印刷動作を制御して印刷部９６から印刷物を出力させる印刷制御部９８とから構成されている。

【００３１】以上の様に構成されたサーバ２０において、ＲＯＭ５０に格納されたプログラムに基づいてＣＰＵ３０が実行する処理につき、以下に説明する。図４は、クライアント１０からサービスの要求を受信した

後、サーバ２０において行われる処理を示すフローチャートである。

【００３２】図４に示すように、サーバ２０は、サービス要求を受けると、その要求された”サービス”に基づいて、サービスＤＢ４４から”認証の種類”を検索し（Ｓ１０）、その結果得られた”認証の種類”に基づいて、認証ＤＢ４２から”認証の有無”を検索する（Ｓ２０）。”認証の有無”は、認証を行うかどうかを判断するためのデータ項目であり、認証ＤＢ４２の検索の結果得られた”認証の有無”に基づいて、認証処理を行うかどうかを判断する（Ｓ３０）。

【００３３】その結果、認証処理を行わないものと判断した場合には（Ｓ３０：ＮＯ）、直ちにサービス提供処理に移行するが（Ｓ８０）、認証処理を行うものと判断した場合には（Ｓ３０：ＹＥＳ）、認証処理を行う（Ｓ４０）。なお、認証処理（Ｓ４０）の詳細については、後述する（図５参照）。

【００３４】認証処理（Ｓ４０）を終えると、認証処理の結果が「ＯＫ」かどうかを判断し（Ｓ５０）、「ＯＫ」でない場合は（Ｓ５０：ＮＯ）、サービスの提供を行わない。一方、認証処理の結果が「ＯＫ」である場合には（Ｓ５０：ＹＥＳ）、リンクキーＤＢ４６の”再提供フラグ”が立っているかどうかを判断する（Ｓ６０）。”再提供フラグ”は、リンクキーの有効期限が切れた場合において、暫定的にサービスの提供を許可するときに立てられるフラグである。

【００３５】”再提供フラグ”が立っていない場合には（Ｓ６０：ＮＯ）、そのままサービス提供処理に移行するが（Ｓ８０）、”再提供フラグ”が立っている場合には、この後に提供するサービスが暫定的なサービス提供であることをクライアント１０のユーザに通知して（Ｓ７０）、サービス提供を行う（Ｓ８０）。

【００３６】なお、ＣＰＵ３０は、Ｓ７０の処理を実行することによって請求項の「通知手段」として機能し、Ｓ８０の処理を実行することによって請求項の「サービス提供手段」として機能する。図５は、サーバ２０で行われる認証処理を示すフローチャートである。

【００３７】認証処理において、サーバ２０は、クライアント１０に対して恒久リンクキーによる認証要求を行い（Ｓ１１０）、その後、クライアント１０が恒久リンクキーを返信してきたかどうかを判断する（Ｓ１２０）。クライアント１０から恒久リンクキーが返信されない場合には（Ｓ１２０：ＮＯ）、恒久リンクキーを新規に作成する（Ｓ１３０）。そして、恒久リンクキーの新規作成が問題なく行われたかどうかを判断し（Ｓ１４０）、所定の問題があった場合には（Ｓ１４０：ＮＯ）、認証処理の結果を「ＮＧ」として（Ｓ１５０）、当該認証処理を終了する。一方、その作成が問題なく行われた場合には（Ｓ１４０：ＹＥＳ）、恒久リンクキーによる認証処理を行う（Ｓ１６０）。なお、”恒久リンクキーの新規作成”の詳細については後述する（図６参照）。

【００３８】クライアント１０から恒久リンクキーが返信された場合には（Ｓ１２０：ＹＥＳ）、直ちに恒久リンクキーによる認証処理を行う（Ｓ１６０）。クライアント１０から送られる恒久リンクキーは、請求項の「認証情報」に相当するものである。なお、恒久リンクキーによる認証処理については後述する（図７参照）。

【００３９】恒久リンクキーによる認証処理（Ｓ１６０）を終えると、その結果が「ＯＫ」であるかどうかを判断し（Ｓ１７０）、「ＯＫ」であれば（Ｓ１７０：ＹＥＳ）、認証結果を「ＯＫ」とし（Ｓ１８０）、その後、当該認証処理を終了する。一方、「ＯＫ」でなければ（Ｓ１７０：ＮＯ）、認証結果を「ＮＧ」とし（Ｓ１５０）、その後、当該認証処理を終了する。

【００４０】図６は、”恒久リンクキーの新規作成”処理を示すフローチャートである。サーバ２０は、要求を受けた”サービス”に基づいて、サービスＤＢ４４から”ＰＩＮコード”を検索し、それに基づいて初期化キーを作成すると共に（Ｓ２１０）、クライアント１０から初期化キーを受信する（Ｓ２２０）。そして、作成した初期化キーに基づいて、受信した初期化キーを認証する（Ｓ２３０）。即ち、初期化キーに基づいて、当該”サービス”への接続についての認証（初期認証という）を行うのである。

【００４１】次に、初期認証の結果が「ＯＫ」かどうかを判断し（Ｓ２４０）、「ＯＫ」でない場合には（Ｓ２４０：ＮＯ）、直ちに当該恒久リンクキー新規作成処理を終了するが、「ＯＫ」である場合には（Ｓ２４０：ＹＥＳ）、要求を受けた”サービス”に基づいて、”サービスＤＢ４４に登録してある”恒久リンクキーの種類”を検索し、その”恒久リンクキーの種類”が”ユニットキー”かどうかを判断する（Ｓ２５０）。

【００４２】その判断の結果、検索された”恒久リンクキーの種類”がユニットキーである場合には（Ｓ２５０：ＹＥＳ）、ユニットキーを生成し（Ｓ２６０）、一方、”恒久リンクキーの種類”がユニットキーでない場合には（Ｓ２５０：ＮＯ）、コンビネーションキーを生成する（Ｓ２７０）。そして、生成したリンクキーを、リンクキーＤＢ４６に登録する（Ｓ２８０）。

【００４３】図７は、サーバ２０において行われる”恒久リンクキーによる認証”処理を示すフローチャートである。この認証処理において、サーバ２０は、クライアント１０の”ＢＤアドレス”に基づいて、リンクキーＤＢ４６からリンクキーを検索し（Ｓ３１０）、リンクキーがあるかどうかを判断する（Ｓ３２０）。

【００４４】ここで、リンクキーがない場合には（Ｓ３２０：ＮＯ）、リンクキーＤＢ４６の再提供フラグをおろすとともに（Ｓ３２５）、恒久リンクキーによる認証の結果を「ＮＧ」として（Ｓ３３０）、当該”恒久リン

クキーによる認証処理”を終了する。

【００４５】一方、リンクキーがある場合には（Ｓ３２０：ＹＥＳ）、そのリンクキーを用いた認証処理を行う（Ｓ３４０）。この認証処理（Ｓ３４０）の結果が「ＯＫ」となるには、受信したリンクキーとリンクキーＤＢ４６に登録されているリンクキーとが一致していること、およびリンクキーＤＢ４６に登録されているリンクキーが有効期限内であることが必要である。リンクキーが有効期限内かどうかについては、認証ＤＢ４２の”有効期限”、リンクキーＤＢ４６の”生成日”および現在の日付に基づいて判断される。

【００４６】この様な認証処理（Ｓ３４０）を終えると、その結果が「ＯＫ」かどうかを判断し（Ｓ３５０）、「ＯＫ」である場合には（Ｓ３５０：ＹＥＳ）、恒久リンクキーによる認証の結果を「ＯＫ」とし（Ｓ３６０）、当該”恒久リンクキーによる認証処理”を終了する。

【００４７】ところで、上記の認証処理の結果が「ＯＫ」でない場合には（Ｓ３５０：ＮＯ）、クライアント１０から受信したリンクキーと、リンクキーＤＢ４６を検索して得られたリンクキーとが一致していたかどうかを判断する（Ｓ３７０）。この判断の結果、両リンクキーが一致していない場合には（Ｓ３７０：ＮＯ）、Ｓ３３０に移行するが、両リンクキーが一致している場合には（Ｓ３７０：ＹＥＳ）、リンクキーＤＢ４６に登録されている恒久リンクキーの有効期限が切れただけであると判断されるので、当該恒久リンクキーに関して、”暫定的な恒久リンクキーの提供設定”を行う。”暫定的な恒久リンクキーの提供設定”とは、恒久リンクキーの有効期限が切れている場合に、所定の条件の下で、暫定的に、その恒久リンクキーを有効なものとみなすためのものであるが、その詳細については後述する（図８参照）。

【００４８】”暫定的な恒久リンクキーの提供設定”（Ｓ３８０）を終えると、暫定的なサービス提供（以下、「再提供」という）をすることができるかどうかを、その処理結果に基づいて判断する（リンクキーＤＢ４６の再提供回数が０回でなく、かつ、リンクキーＤＢ４６の再提供有効期限が０日でない場合にのみ、再提供が許可される）（Ｓ３９０）。そして、再提供できない場合には（Ｓ３９０：ＮＯ）、Ｓ３３０に移行するが、再提供できる場合には（Ｓ３９０：ＹＥＳ）、リンクキーＤＢ４６において当該”恒久リンクキー”に対応する”再提供フラグ”を立て（Ｓ４００）、その後、Ｓ３６０に移行する。

【００４９】なお、ＣＰＵ３０は、Ｓ３４０～Ｓ３６０の処理を実行することにより、請求項の「認証手段」として機能し、Ｓ３７０～Ｓ４００の処理を実行することにより、請求項の「暫定サービス提供手段」としての機能する。また、リンクキーＤＢ４６には、有効期限内の恒久リンクキーおよび有効期限切れの恒久リンクキーの両方が記録されているのであるが、有効期限内の”恒久リンクキー”が、請求項における「現在の照合情報」に相当し、有効期限を過ぎた”恒久リンクキー”が、請求項における「過去の照合情報」に相当するものである。

【００５０】図８は、”暫定的な恒久リンクキーの提供設定”処理を示すフローチャートである。本処理においては、”再提供フラグ”が立っているかどうかを、リンクキーＤＢ４６を検索して判断する（Ｓ５１０）。”再提供フラグ”が立っている場合には（Ｓ５１０：ＹＥＳ）、リンクキーＤＢ４６の”再提供回数”を１減らし（Ｓ５２０）、直ちに”暫定的な恒久リンクキーの提供設定”処理を終了する。

【００５１】一方、”再提供フラグ”が立っていない場合には（Ｓ５１０：ＮＯ）、Ｓ１０で検索された”認証の種類”に対応する”無効時の対応（回数）”が「ＮＧ」となっているかどうかを、認証ＤＢ４２を検索して判断する（Ｓ５３０）。ここで、「ＮＧ」である場合には（Ｓ５３０：ＹＥＳ）、リンクキーＤＢ４６の”再提供回数”を「０」とする（Ｓ５４０）と共に、”再提供有効期限”を「０」とし（Ｓ５５０）、当該”暫定的な恒久リンクキーの提供設定”を終了する。

【００５２】また、認証ＤＢ４２の”無効時の対応（回数）”が、「ＮＧ」でない場合には（Ｓ５３０：ＮＯ）、リンクキーＤＢ４６の”再提供回数”に、認証ＤＢ４２の”無効時の対応（回数）”のデータを設定し（Ｓ５６０）、そして、認証ＤＢ４２の”無効時の対応（期限）”が「ＮＧ」かどうかを判断する（Ｓ５７０）。その結果、認証ＤＢ４２の”無効時の対応（期限）”が「ＮＧ」である場合には（Ｓ５７０：ＹＥＳ）、Ｓ５５０に移行し、「ＮＧ」でない場合には（Ｓ５７０：ＮＯ）、リンクキーＤＢ４６の”再提供有効期限”に、認証ＤＢ４２の”無効時の対応（期限）”のデータを設定し（Ｓ５８０）、その後、当該”暫定的な恒久リンクキーの提供設定”を終了する。

【００５３】つまり、認証ＤＢ４２の”無効時の対応（回数）”および”無効時の対応（期限）”とサービスＤＢ４４の”サービス”とは、”認証の種類”に基づいて関連づけられ、これにより、サーバ２０が提供可能な”サービス”ごとに暫定的なサービス提供の可否（条件）が設定されている。そして、その条件の下で、暫定的なサービスの提供が行われるのである。

【００５４】以上の様に、本実施例のサービス提供システムにおいて、サーバ２０は、クライアント１０から取得した恒久リンクキーと自己の認証ＤＢ４２に登録されている恒久リンクキーとに基づいて、クライアント１０に対する認証処理（Ｓ３４０）を行った結果、有効期限内の恒久リンクキーによってクライアント１０が認証されない場合であっても（Ｓ３５０：ＮＯ）、有効期限切れの恒久リンクキーによって認証される場合には（Ｓ３

７０：ＹＥＳ）、所定の条件の下で、暫定的にサービスを提供する（Ｓ３９０：ＹＥＳ）。これにより、サービス要求に対する柔軟な対応が実現され、利用者側がサービスを利用し易くなる。

【００５５】また、暫定的なサービスを提供する際（Ｓ６０：ＹＥＳ）、所定の情報、即ち暫定的なサービス提供であることをクライアント１０のユーザに通知して注意を促すため、サービスがより利用しやすくなる。また、暫定的なサービスの提供可否を、サービス毎に設定しているため、サービス提供システムを柔軟性に運用することができる。

【００５６】以上、本発明の一実施例について説明したが、本発明は上記実施例に限定されるものではなく、種々の態様をとることができる。例えば、上記実施例では、暫定的なサービスを提供する条件として、回数および期間に制限を設けたが、これに限られるものではない。サービスの内容に応じて、回数のみを制限するようにしてもよいし、また期間のみに制限を設けてもよい。

【００５７】また、上記実施例では、Ｂｌｕｅｔｏｏｔｈ方式により、クライアント１０とサーバ２０とが無線通信を行うものとして説明したが、これに限られるものではない。更に、上記実施例では、リンクキーの一致及びリンクキーの有効性（有効期限内であること）に基づいて認証処理を行い（Ｓ４０）、共に条件を満たす場合に認証処理ＯＫとする例を挙げて説明したが、リンクキーの有効性（有効期限内であること）については、検討しない構成としても良い。つまり、リンクキーの一致・不一致に基づいて認証処理を行う構成としても良い。この場合、過去のリンクキー（過去の照合情報）をリンクキーＤＢに記憶しておき、現在のリンクキー（現在の照合情報）と一致しなくても、過去のリンクキーと一致する場合に、暫定的なサービスを提供する構成となる。このような構成によれば、管理者によって定期的、あるいは不規則に認証の種類を変えたとしても、その変更前のユーザに対しては、少なくとも暫定的なサービスが提供されることとなるため、セキュリティの向上とユーザに対する利便性とをうまく両立させることが可能である。

【図面の簡単な説明】

【図１】　一実施例としてのサービス提供システム１の構成を示す図である。

【図２】　サーバの構成を示すブロック図である。

【図３】　（ａ）は認証データベースの内容、（ｂ）はサービスデータベースの内容、（ｃ）はリンクキーデータベースの内容を示す図である。

【図４】　サービス要求を受けた後にサーバで行われる処理を示すフローチャートである。

【図５】　サーバで行われる認証処理を示すフローチャートである。

【図６】　サーバで行われる恒久リンクキーの新規作成処理を示すフローチャートである。

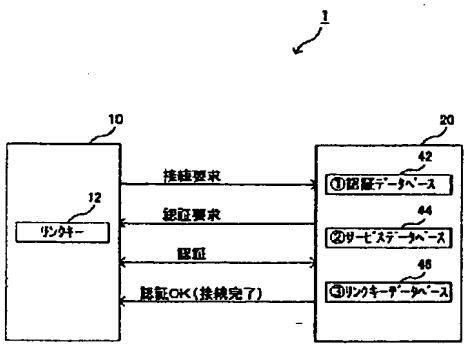
【図７】　サーバで行われる恒久リンクキーによる認証処理を示すフローチャートである。

【図８】　サーバで行われる暫定的な恒久リンクキーの提供設定処理を示すフローチャートである。

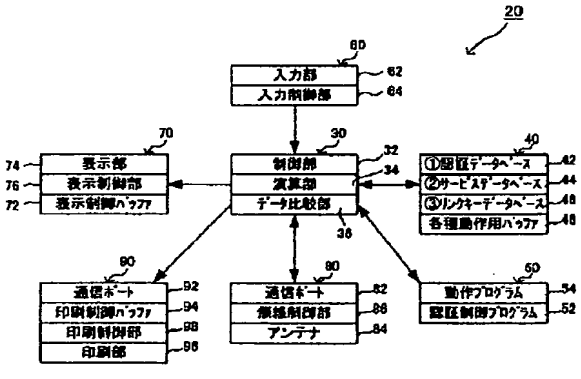
【符号の説明】

１…サービス提供システム
１０…クライアント装置
２０…サーバ装置　３０…ＣＰＵ
４０…ＲＡＭ　５０…ＲＯＭ
４２…認証ＤＢ　４４…サービスＤＢ
４６…リンクキーＤＢ

【図１】



【図２】



【図３】

(a) 認証データベース

認証の種類	認証1	認証2	認証3
認証の有無	行わない	行う	行う
有効期限	NG	14日	30日
無効時の対応(回数)	NG	NG	+M回
無効時の対応(期限)	NG	NG	10日

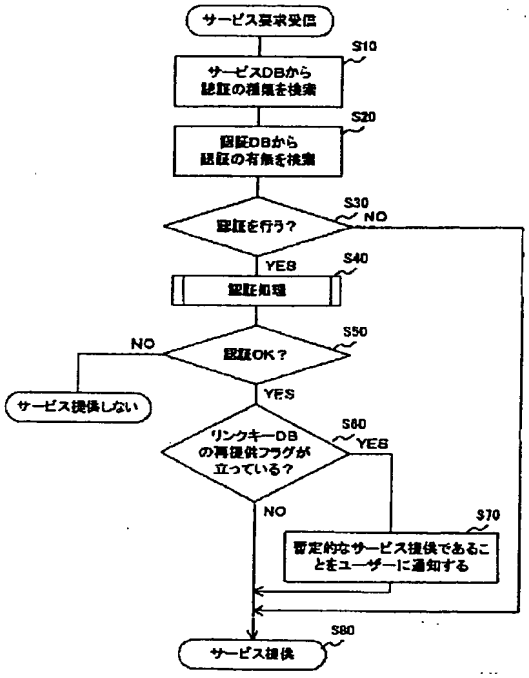
(b) サービスデータベース

サービス	サービスA(プリント)	サービスB(FAX)	サービスC(***)
認証の種類	認証3	認証2	認証1
PINコード	***	なし	****
恒久リンクキーの種類	コンビネーション	ユニット	コンビネーション

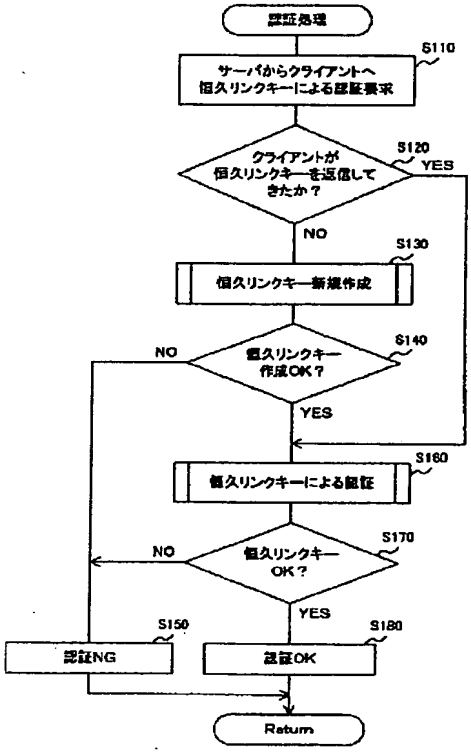
(c) リンクキーデータベース

恒久リンクキー	リンクキー1	リンクキー2
恒久リンクキーの種類	コンビネーション	コンビネーション
BD_ADDR	*******	*******
生成日	****	***
再提供回数	0	M
再提供有効期限	0	10日
再提供フラグ	0	1

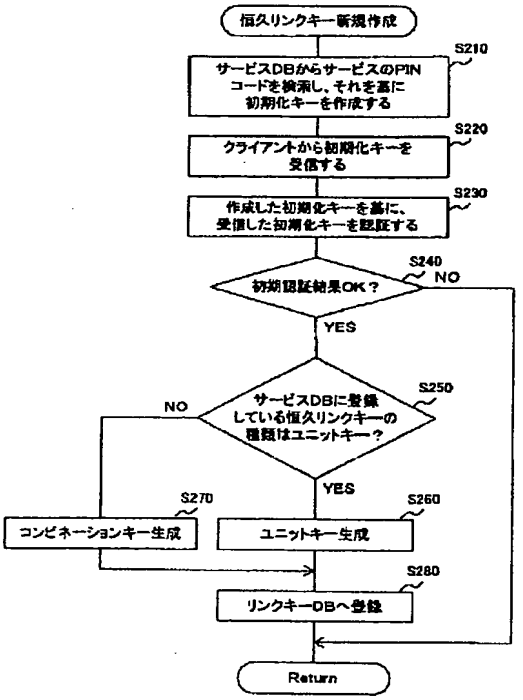
【図４】



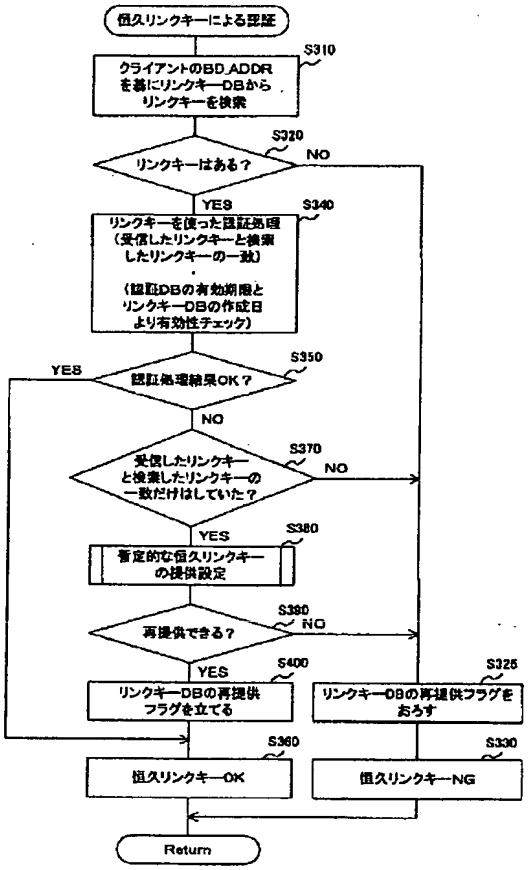
【図５】



【図６】



【図７】



【図８】